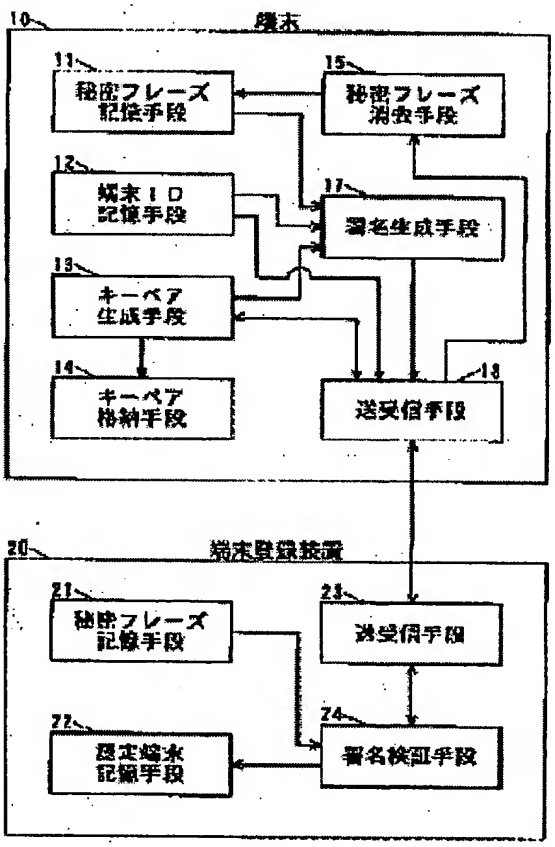
Publication number: JP2002297548
Publication date: 2002-10-11
Inventor: NAKANISHI TAKAHIRO; HATANO KOJI; SUGIURA MASAKI; TSUKAMOTO YOSHIHIRO
Applicant: MATSUSHITA ELECTRIC IND CO LTD
Classification:
- international: ***B42D15/10; G06F12/14; G06F15/00; G06F21/20; G06F21/24; G06Q10/00; H04L9/32;*** **B42D15/10; G06F12/14; G06F15/00; G06F21/00; G06F21/20; G06Q10/00; H04L9/32;** (IPC1-7): G06F15/00; B42D15/10; G06F12/14; G06F17/60; H04L9/32
- european:
Application number: JP20010100234 20010330
Priority number(s): JP20010100234 20010330

Abstract of **JP2002297548**

PROBLEM TO BE SOLVED: To provide a registration system which is capable of discriminating a produced terminal with another company's product, and also registering so as to be identified on a network individually. SOLUTION: In a terminal 10, there are provided a key pair generating means 13 for generating a key pair of public key and secret key, a secret phrase storage means 11 for storing a secret phrase necessary for registration, and a signature generating means 17 for generating signature data encoded by the secret key using terminal identification information, the public key and secret phrase. Registration request data including the terminal identification information, public key and signature data are transmitted to a terminal registration device 20. The terminal registration device comprises: a signature verification means 24 for extracting the terminal identification information and public key from the registration request data, and reading the secret phrase from a secret phrase memory means 21 to verify the signature data; and an authorization terminal storage means 22 for storing the terminal identification information and the public key which are validated by the signature verification means. The terminal registration device can be discriminated with another company's product depending on whether the terminal knows the secret phrase.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2002－297548
（P2002－297548A）
(43)公開日　平成14年10月11日(2002.10.11)

(51)Int.Cl.⁷		識別記号	FI		テーマコード（参考）
G06F	15/00	330	G06F	15/00	330C　2C005
B42D	15/10	521	B42D	15/10	521　5B017
G06F	12/14	320	G06F	12/14	320F　5B085
	17/60	176		17/60	176A　5J104
H04L	9/32		H04L	9/00	673B

審査請求　未請求　請求項の数21　ＯＬ　（全 12 頁）　最終頁に続く

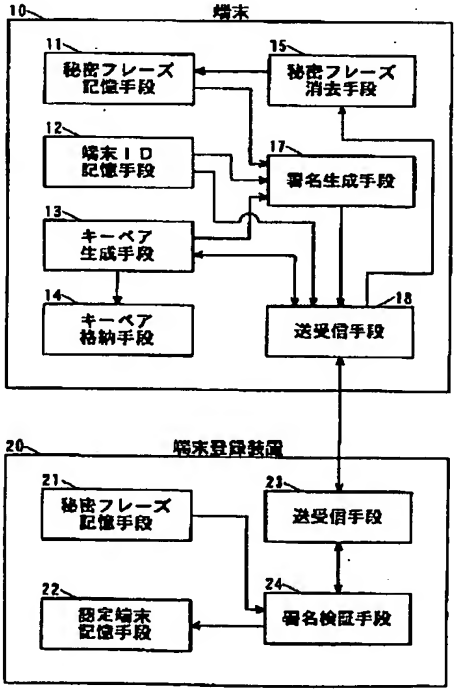
(21)出願番号　特願2001－100234(P2001－100234)
(22)出願日　平成13年３月30日(2001.3.30)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　中西　隆博
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　幡野　浩司
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100099254
弁理士　役　昌明　（外３名）

最終頁に続く

(54)【発明の名称】　端末登録システムとそれを構成する装置及び方法

(57)【要約】
【課題】　製造した端末を、他社製品と区別して、且つ、ネットワーク上で個別に識別できるように登録する登録システムを提供する。
【解決手段】　端末10に、公開鍵・秘密鍵のキーペアを生成するキーペア生成手段13と、登録を行うために必要な秘密フレーズを格納する秘密フレーズ記憶手段11と、端末識別情報、公開鍵、秘密フレーズを用い、秘密鍵で暗号化して署名データを生成する署名生成手段17とを設け、端末識別情報、公開鍵及び署名データを含む登録要請データを端末登録装置20に送信する。端末登録装置は、登録要請データから端末識別情報と公開鍵とを取り出し、秘密フレーズ記憶手段21から秘密フレーズを読み出し、署名データを検証する署名検証手段24と、署名検証手段が有効と認めた端末識別情報と公開鍵とを記憶する認定端末記憶手段22とを設ける。端末登録装置は、端末が秘密フレーズを知っているか否かにより、他社製品と区別できる。



【特許請求の範囲】

【請求項１】　端末を、ネットワークを経由して端末登録装置に登録する端末登録システムであって、

前記端末は、

秘密フレーズを格納する秘密フレーズ記憶手段を備え、

公開鍵・秘密鍵のキーペアを生成し、前記秘密フレーズと前記公開鍵と端末識別情報とのデータを基に、前記秘密鍵で暗号化した署名データを生成して、前記署名データと前記端末識別情報と前記公開鍵とを含む登録確認データを端末登録装置に送信し、

前記端末登録装置は、

前記秘密フレーズを格納する秘密フレーズ記憶手段を備え、

前記秘密フレーズ記憶手段から読み出した前記秘密フレーズを用いて、前記登録確認データに含まれる前記署名データを検証し、署名を有効と認めた場合に前記端末識別情報と前記公開鍵とを登録して、前記端末に登録確認データを返信することを特徴とする端末登録システム。

【請求項２】　端末を、ネットワークを経由して端末登録装置に登録する端末登録システムであって、

前記端末は、

秘密フレーズを格納する秘密フレーズ記憶手段を備え、

公開鍵・秘密鍵のキーペアを生成し、前記公開鍵と端末識別情報とのデータを基に、前記秘密鍵で暗号化した署名データを生成し、前記署名データと前記端末識別情報と前記公開鍵とを含む登録確認データを前記秘密フレーズで暗号化して端末登録装置に送信し、

前記端末登録装置は、

前記秘密フレーズを格納する秘密フレーズ記憶手段を備え、

前記秘密フレーズ記憶手段から読み出した前記秘密フレーズを用いて、暗号化されている前記登録確認データを復号化した後、前記登録確認データに含まれる前記署名データを検証し、署名を有効と認めた場合に前記端末識別情報と前記公開鍵とを登録して、前記端末に登録確認データを返信することを特徴とする端末登録システム。

【請求項３】　端末を、ネットワークを経由して端末登録装置に登録する端末登録システムであって、

前記端末は、

公開鍵・秘密鍵のキーペアを生成するキーペア生成手段と、

前記キーペアのうち、少なくとも秘密鍵を外部から参照できない場所に格納するキーペア格納手段と、

登録を行うために必要な秘密フレーズを外部から参照できない場所に格納する秘密フレーズ記憶手段と、

端末識別情報を記録する端末識別情報記憶手段と、

前記端末識別情報と前記公開鍵と秘密フレーズとの一方向性ハッシュ値に対して、前記秘密鍵で暗号化した署名データを生成する署名生成手段と、

前記端末識別情報、前記公開鍵、及び前記署名データを含む登録要請データを前記端末登録装置に送信し、登録確認データを受信する送受信手段とを備え、

前記端末登録装置は、

前記登録要請データを受信し、前記登録確認データを送信する送受信手段と、

前記秘密フレーズを記憶する秘密フレーズ記憶手段と、

前記登録要請データから前記端末識別情報と前記公開鍵とを取り出し、前記秘密フレーズ記憶手段から秘密フレーズを読み出し、前記端末識別情報と前記公開鍵と前記秘密フレーズとの一方向性ハッシュ値を計算し、その値と前記署名データを前記公開鍵で復号したときのデータとが一致しているかどうか判定する署名検証手段と、

前記署名検証手段が有効と認めた前記端末識別情報と前記公開鍵とのペアを記憶する認定端末記憶手段とを備えることを特徴とする端末登録システム。

【請求項４】　端末を、ネットワークを経由して端末登録装置に登録する端末登録システムであって、

前記端末は、

公開鍵・秘密鍵のキーペアを生成するキーペア生成手段と、

前記キーペアのうち、少なくとも秘密鍵を外部から参照できない場所に格納するキーペア格納手段と、

登録を行うために必要な秘密のフレーズを外部から参照できない場所に格納する秘密フレーズ記憶手段と、

端末識別情報を記録する端末識別情報記憶手段と、

前記端末識別情報と前記公開鍵との一方向性ハッシュ値に対して、前記秘密鍵で暗号化した署名データを生成する署名生成手段と、

前記端末識別情報、前記公開鍵、及び前記署名データを含む登録要請データを前記秘密フレーズで暗号化し、前記端末登録装置に送信し、登録確認データを受信する送受信手段とを備え、前記端末登録装置は、

前記暗号化された登録要請データを受信し、前記登録確認データを送信する送受信手段と、

前記秘密フレーズを記憶する秘密フレーズ記憶手段と、

前記暗号化された登録要請データを前記秘密フレーズで復号化し、前記端末識別情報と前記公開鍵とを取り出して、その一方向性ハッシュ値を計算し、その値と前記署名データを前記公開鍵で復号したときのデータとが一致しているかどうか判定する署名検証手段と、

前記署名検証手段が有効と認めた前記端末識別情報と前記公開鍵とのペアを記憶する認定端末記憶手段とを備えることを特徴とする端末登録システム。

【請求項５】　前記端末が、登録完了を示す前記登録確認データを受信したとき、前記秘密フレーズ記憶手段から秘密フレーズを消去することを特徴とする請求項１から４のいずれかに記載の端末登録システム。

【請求項６】　前記登録確認データが、前記端末識別情報と、前記公開鍵と、前記公開鍵及び端末識別情報のデータを基に端末登録装置の秘密鍵で暗号化した端末登録

装置の署名データとを備えることを特徴とする請求項１から５のいずれかに記載の端末登録システム。

【請求項７】　端末を、ネットワークを経由して端末登録装置に登録する端末登録方法であって、
前記端末が公開鍵と秘密鍵とからなるキーペアを生成する第一のステップと、
前記端末の端末識別情報と前記公開鍵と秘密フレーズとの一方向性ハッシュ値に対して、前記秘密鍵で暗号化した署名データを生成する第二のステップと、
前記端末識別情報、前記公開鍵及び前記署名データを含む登録要請データを生成する第三のステップと、
前記登録要請データを端末登録装置に送信する第四のステップと、
前記端末登録装置が前記登録要請データを受信する第五のステップと、
前記登録要請データから前記端末識別情報と前記公開鍵とを取り出し、それらと前記秘密フレーズとの一方向性ハッシュ値を計算し、その値と前記署名データを前記公開鍵で復号したときのデータとが一致しているかどうかを判定する第六のステップと、
一致した場合に前記端末識別情報と前記公開鍵とのペアを記憶する第七のステップと、
登録完了を示す前記登録確認データを端末に返信する第八のステップと、
前記端末が前記端末登録装置から返信される登録確認データを受信する第九のステップと、
前記登録確認データが登録完了を示す情報である場合、前記キーペアをキーペア格納手段に格納する第十のステップとから成ることを特徴とする端末登録方法。

【請求項８】　端末を、ネットワークを経由して端末登録装置に登録する端末登録方法であって、
前記端末が公開鍵と秘密鍵とからなるキーペアを生成する第一のステップと、
前記端末の端末識別情報と前記公開鍵との一方向性ハッシュ値に対して、前記秘密鍵で暗号化した署名データを生成する第二のステップと、
前記端末識別情報、前記公開鍵及び前記署名データを含む登録要請データを生成し、前記登録要請データを秘密フレーズで暗号化する第三のステップと、
暗号化した前記登録要請データを端末登録装置に送信する第四のステップと、
前記端末登録装置が暗号化された前記登録要請データを受信する第五のステップと、
暗号化された前記登録要請データを前記秘密フレーズで復号化する第六のステップと、
前記登録要請データから前記端末識別情報と前記公開鍵とを取り出し、それらの一方向性ハッシュ値を計算し、その値と前記署名データを前記公開鍵で復号したときのデータとが一致しているかどうかを判定する第七のステップと、
一致した場合に前記端末識別情報と前記公開鍵とのペアを記憶する第八のステップと、
登録完了を示す前記登録確認データを端末に返信する第九のステップと、
前記端末が前記端末登録装置から返信される登録確認データを受信する第十のステップと、
前記登録確認データが登録完了を示す情報である場合、前記キーペアをキーペア格納手段に格納する第十一のステップとから成ることを特徴とする端末登録方法。

【請求項９】　ネットワークを介して接続する端末登録装置に登録される端末であって、
公開鍵・秘密鍵のキーペアを生成するキーペア生成手段と、
前記キーペアのうち、少なくとも秘密鍵を外部から参照できない場所に格納するキーペア格納手段と、
登録を行うために必要な秘密フレーズを外部から参照できない場所に格納する秘密フレーズ記憶手段と、
端末識別情報を記録する端末識別情報記憶手段と、
前記端末識別情報と前記公開鍵と前記秘密フレーズとの一方向性ハッシュ値に対して、前記秘密鍵で暗号化した署名データを生成する署名生成手段と、
前記端末識別情報、前記公開鍵及び前記署名データを含む登録要請データを前記端末登録装置に送信し、登録確認データを受信する送受信手段とを備えることを特徴とする端末。

【請求項１０】　ネットワークを介して接続する端末登録装置に登録される端末であって、
公開鍵・秘密鍵のキーペアを生成するキーペア生成手段と、
前記キーペアのうち、少なくとも秘密鍵を外部から参照できない場所に格納するキーペア格納手段と、
登録を行うために必要な秘密のフレーズを外部から参照できない場所に格納する秘密フレーズ記憶手段と、
端末識別情報を記録する端末識別情報記憶手段と、
前記端末識別情報と前記公開鍵との一方向性ハッシュ値に対して、前記秘密鍵で暗号化した署名データを生成する署名生成手段と、
前記端末識別情報、前記公開鍵、及び前記署名データを含む登録要請データを前記秘密フレーズで暗号化し、前記端末登録装置に送信し、登録確認データを受信する送受信手段とを備えることを特徴とする端末。

【請求項１１】　登録完了後に前記秘密フレーズ記憶手段から秘密フレーズを消去する秘密フレーズ消去手段を備えることを特徴とする請求項９または１０に記載の端末。

【請求項１２】　前記登録確認データに添えられた前記端末登録装置の証明書を格納する証明書記憶手段を備えることを特徴とする請求項９、１０または１１に記載の端末。

【請求項１３】　前記端末が、電話機、ＦＡＸ、コピー

機、テレビ、ビデオ、ＳＴＢ、冷蔵庫、電子レンジ、ＩＣカード、ＰＣ、プリンタ、ジャーポット、食器洗い機、洗濯機、湯沸かし機、照明、自動ドア、自販機、エレベータ、ゲーム機、音楽再生装置、扇風機、エアコン、ヒーター、ガスコンロ、自転車、車、バイク、カーナビ、掃除機、アイロンのいずれか、またはそれらの複合機であることを特徴とする請求項９から１０のいずれかに記載の端末。

【請求項１４】　ネットワークを介して接続する端末を登録する端末登録装置であって、
端末から登録要請データを受信し、前記端末に登録確認データを送信する送受信手段と、
秘密フレーズを記憶する秘密フレーズ記憶手段と、
前記登録要請データから端末識別情報と公開鍵とを取り出し、前記秘密フレーズ記憶手段から秘密フレーズを読み出し、前記端末識別情報と前記公開鍵と前記秘密フレーズとの一方向性ハッシュ値を計算し、その値と前記登録要請データに含まれる署名データを前記公開鍵で復号したときのデータとが一致しているかどうか判定する署名検証手段と、
前記署名検証手段が有効と認めた前記端末識別情報と前記公開鍵とのペアを記憶する認定端末記憶手段とを備えることを特徴とする端末登録装置。

【請求項１５】　ネットワークを介して接続する端末を登録する端末登録装置であって、
端末から暗号化された登録要請データを受信し、前記端末に登録確認データを送信する送受信手段と、
秘密フレーズを記憶する秘密フレーズ記憶手段と、
前記暗号化された登録要請データを前記秘密フレーズで復号化し、得られた前記登録要請データから端末識別情報と公開鍵とを取り出して、前記端末識別情報と前記公開鍵との一方向性ハッシュ値を計算し、その値と前記登録要請データに含まれる署名データを前記公開鍵で復号したときのデータとが一致しているかどうか判定する署名検証手段と、
前記署名検証手段が有効と認めた前記端末識別情報と前記公開鍵とのペアを記憶する認定端末記憶手段とを備えることを特徴とする端末登録装置。

【請求項１６】　前記署名検証手段が有効と認めた前記端末識別情報と前記公開鍵とを用いて、前記端末識別情報と、前記公開鍵と、前記端末識別情報及び前記公開鍵の一方向性ハッシュ値に対して端末登録装置の秘密鍵で暗号化した署名データとを含む証明書を生成する証明書生成手段を備えることを特徴とする請求項１４または１５に記載の端末登録装置。

【請求項１７】　ネットワークを介して接続する端末登録装置に登録される端末が保持するプログラムであって、
コンピュータを、
公開鍵・秘密鍵のキーペアを生成するキーペア生成手段と、
登録を行うために必要な秘密フレーズが格納された秘密フレーズ記憶手段から前記秘密フレーズを読み出し、端末識別情報と前記公開鍵と前記秘密フレーズとの一方向性ハッシュ値を計算し、前記ハッシュ値に対して、前記秘密鍵で暗号化して署名データを生成する署名生成手段と、
前記端末識別情報、前記公開鍵及び前記署名データを含む登録要請データを前記端末登録装置に送信し、前記端末登録装置から登録確認データを受信する送受信手段として機能させるためのプログラム。

【請求項１８】　ネットワークを介して接続する端末登録装置に登録される端末が保持するプログラムであって、
コンピュータを、
公開鍵・秘密鍵のキーペアを生成するキーペア生成手段と、
端末識別情報と前記公開鍵との一方向性ハッシュ値を計算し、前記ハッシュ値に対して、前記秘密鍵で暗号化して署名データを生成する署名生成手段と、
登録を行うために必要な秘密フレーズが格納された秘密フレーズ記憶手段から前記秘密フレーズを読み出し、前記端末識別情報、前記公開鍵、及び前記署名データを含む登録要請データを前記秘密フレーズで暗号化し、前記端末登録装置に送信し、前記端末登録装置から登録確認データを受信する送受信手段として機能させるためのプログラム。

【請求項１９】　ネットワークを介して接続する端末を登録する端末登録装置が保持するプログラムであって、
コンピュータを、
端末から登録要請データを受信し、前記端末に登録確認データを送信する送受信手段と、
前記登録要請データから端末識別情報と公開鍵とを取り出し、秘密フレーズが格納された秘密フレーズ記憶手段から秘密フレーズを読み出し、前記端末識別情報と前記公開鍵と前記秘密フレーズとの一方向性ハッシュ値を計算し、その値と前記登録要請データに含まれる署名データを前記公開鍵で復号したときのデータとが一致しているかどうか判定する署名検証手段として機能させるためのプログラム。

【請求項２０】　ネットワークを介して接続する端末を登録する端末登録装置が保持するプログラムであって、
コンピュータを、
端末から暗号化された登録要請データを受信し、前記端末に登録確認データを送信する送受信手段と、
秘密フレーズが格納された秘密フレーズ記憶手段から秘密フレーズを読み出し、前記暗号化された登録要請データを前記秘密フレーズで復号化し、得られた前記登録要請データから端末識別情報と公開鍵とを取り出して、前記端末識別情報と前記公開鍵との一方向性ハッシュ値を

計算し、その値と前記登録要請データに含まれる署名データを前記公開鍵で復号したときのデータとが一致しているかどうか判定する署名検証手段として機能させるためのプログラム。

【請求項２１】　コンピュータを、さらに、
前記署名検証手段が有効と認めた前記端末識別情報及び前記公開鍵の一方向性ハッシュ値を計算し、前記ハッシュ値を端末登録装置の秘密鍵で暗号化して署名データを生成し、前記端末識別情報と、前記公開鍵と、前記署名データとを含む証明書を生成する証明書生成手段として機能させるための請求項１９または２０に記載のプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、通信機能を持つ端末をネットワーク上で特定できるように登録する登録システムと、それを構成する装置及び方法に関し、特に、デジタル家電などの登録に広く適用できる方式の確立を図るものである。

【０００２】

【従来の技術】近年、ネットワークを利用した情報やサービスの提供が急速に増加しており、ユーザは、例えば、音楽配信サービスに加入することにより、ネットワークを通じて配信される音楽を自身の端末に蓄積して楽しむことができる。

【０００３】現在、家電製品のＩＴ化が進み、通信機能を持つ冷蔵庫や電子レンジなどが続々登場している状況にあるため、ネットワークを利用するサービス提供は、今後、益々増えることが確実である。また、それに伴い、こうしたデジタル家電を製造するメーカーでは、自社の製品に特化したネットワークサービスを提供し、他社製品との差別化を図る動きが拡大している。

【０００４】ネットワークを利用するシステムでは、通信の相手が本人であることを確認する必要があり、そのため、通信開始時に認証の手順が取られる。認証には、信頼できる第三者機関を利用する方式と、第三者機関の援助を得ずに、相互認証する方式とがある。

【０００５】第三者機関を利用する一般的な方式では、申請者が端末からオンラインで認証機関に証明書発行を要求する。これに対して、認証機関は審査を行った後、認証機関のデジタル署名を付した証明書を発行する。申請者は、端末からサーバにサービスを求める場合、この証明書を添えてサーバにアクセスする。サーバは、証明書によりユーザを認証し、また、必要があれば、認証機関にユーザの確認を求める。

【０００６】認証機関は、その審査において、端末が、その端末にしか知り得ないことを知っているかどうかを確認した上で証明書を発行する。具体的には、端末は、公開鍵と秘密鍵のペア（キーペア）を生成して、公開鍵を秘密鍵で暗号化し、この暗号化した公開鍵に、暗号化していない公開鍵を添えて認証機関に転送する。認証機関では、秘密鍵で暗号化された公開鍵を、添付された公開鍵で復号化し、復号化した公開鍵と添付された公開鍵とが一致するか否かを調べる。一致すれば、申請した端末は、その端末にしか知り得ない秘密鍵を知っていることになる。この一致を確認した認証機関は、公開鍵を保管し、端末に証明書を発行する。

【０００７】図１１は、従来のＷｅｂブラウザ用の証明書取得手順（Lincoln D.Stein著、株式会社クイック訳「Ｗｅｂセキュリティガイド」株式会社アスキー発行、PP.46,102～110）を示している。証明書希望者は、キーペアを生成し、秘密鍵で暗号化した公開鍵と、暗号化していない公開鍵とを含む証明書発行要求を生成して、オンラインで認証機関に転送する。また、証明書希望者は、別途、代金を銀行に振り込み、その振り込みの控えと、個人証明書情報（免許証のコピーなど）とを認証機関に郵送する。認証機関は、審査を行い、審査をパスすれば、公開鍵を保管し、端末には、認証機関のデジタル署名を付した証明書を電子メールで送る。端末は、この証明書をブラウザにインストールする。

【０００８】デジタル署名は、良く知られているように、メッセージ（証明書の内容）をハッシュ関数で圧縮し、このハッシュ値を秘密鍵で暗号化して生成される。このデジタル署名をメッセージに添付することにより、署名者の公開鍵を知る人は、デジタル署名を公開鍵で復号化して得られるハッシュ値と、メッセージから算出したハッシュ値との同一性を調べることにより、その署名の正当性を検証することができる。

【０００９】また、図１２は、製造したＩＣカードにキーペアを登録するために行われている従来の手順を示している。

【００１０】ＩＣカード製造工場で製造したキーペア未記入の新しいＩＣカードをサービス事業者（カード会社）のもとに運び、ここで生成したキーペアを、リーダー／ライターでＩＣカードに書き込む。次いで、公開鍵出力コマンドを実行し、ＩＣカードから出力された公開鍵をサーバに登録する。この登録されたキーペアを持つＩＣカードがカード利用者に配布される。

【００１１】

【発明が解決しようとする課題】しかし、従来のこれらの方式は、メーカーが、自社製品のデジタル家電などをネットワーク上で識別できるように登録する登録方法としては、適切なものではない。

【００１２】メーカーが工場に特別の装置を用意して、製品の端末を個々に登録してから出荷したり、登録事業者のもとに家電製品を持ち込み、登録した後に顧客に届けるような形態は、作業負担が増えるため適切ではない。

【００１３】また、個々の端末から認定機関に登録を申請する従来の方式は、審査する側で、自社の製品である

ことを特定できない（即ち、キーペアの生成機能を持つ端末であれば、どこの製品であっても登録できる）ため、自社製品の登録方法には適用することができない。

【００１４】また、自社製品に共通のグローバルシークレットを持たせて自社製品を識別する方式も従来から検討されているが、この方式では、グローバルシークレットが解読されて不正利用された場合の被害が大きいと云う問題点がある。また、グローバルシークレットを使用する方式では、端末を個別に識別することができないため、端末の認定を個々に取り消したりすることが不可能である。

【００１５】本発明は、こうした従来の問題点を解決するものであり、製造した端末を、他社製品と区別して、且つ、ネットワーク上で個別に識別できるように登録する効率的な登録システムを提供し、また、それを構成する装置及び方法を提供することを目的としている。

【００１６】

【課題を解決するための手段】そこで、本発明では、端末を、ネットワークを経由して端末登録装置に登録する端末登録システムにおいて、端末には、秘密フレーズを格納する秘密フレーズ記憶手段を設け、公開鍵・秘密鍵のキーペアを生成し、秘密フレーズと公開鍵と端末識別情報とのデータを基に、秘密鍵で暗号化した署名データを生成して、この署名データと端末識別情報と公開鍵とを含む登録確認データを端末登録装置に送信し、端末登録装置には、秘密フレーズを格納する秘密フレーズ記憶手段を設け、秘密フレーズ記憶手段から読み出した秘密フレーズを用いて、登録確認データに含まれる署名データを検証し、署名を有効と認めた場合に端末識別情報と公開鍵とを登録して、端末に登録確認データを返信するように構成している。

【００１７】また、端末には、秘密フレーズを格納する秘密フレーズ記憶手段を設け、公開鍵・秘密鍵のキーペアを生成し、公開鍵と識別情報とのデータを基に、秘密鍵で暗号化した署名データを生成し、この署名データと端末識別情報と公開鍵とを含む登録確認データを秘密フレーズで暗号化して端末登録装置に送信し、端末登録装置には、秘密フレーズを格納する秘密フレーズ記憶手段を設け、秘密フレーズ記憶手段から読み出した秘密フレーズを用いて、暗号化されている登録確認データを復号化した後、登録確認データに含まれる署名データを検証し、署名を有効と認めた場合に端末識別情報と公開鍵とを登録して、端末に登録確認データを返信するように構成している。

【００１８】そのため、端末登録装置は、端末が秘密フレーズを知っていることを確認することにより、他社製品と区別して、且つ、ネットワーク上で個別に識別できる形で登録することができる。

【００１９】

【発明の実施の形態】（第１の実施形態）本発明の実施形態における端末登録システムでは、工場で製造された端末に秘密のフレーズが格納され、端末を登録する端末登録装置（登録サーバ）は、端末が秘密のフレーズを知っていることを確認して、その端末を登録する。

【００２０】図１は、登録を受ける端末10と、端末10と通信回線で接続し、端末を登録する端末登録装置20との構成を示している。端末10は、公開鍵・秘密鍵のキーペアを生成するキーペア生成手段13と、秘密のフレーズを格納する不揮発性ＲＡＭから成る秘密フレーズ記憶手段11と、端末識別情報（端末ＩＤ）を記憶する端末ＩＤ記憶手段12と、キーペアを格納するキーペア格納手段14と、端末ＩＤと公開鍵と秘密フレーズとの一方向性ハッシュ値に対して、秘密鍵で暗号化した署名データを生成する署名生成手段17と、端末ＩＤ、公開鍵及び署名データを含む登録要請データを端末登録装置20に送信し、登録確認データを受信する送受信手段18と、登録完了後に秘密フレーズを消去する秘密フレーズ消去手段15とを備えている。

【００２１】また、端末登録装置20は、端末10から登録要請データを受信し、登録確認データを送信する送受信手段23と、登録要請データから端末ＩＤと公開鍵とを取り出し、それらと秘密フレーズとの一方向性ハッシュ値を計算し、その値と署名データを公開鍵で復号したときのデータとが一致しているかどうかを判定する署名検証手段24と、秘密フレーズを記憶する秘密フレーズ記憶手段21と、署名検証手段24が有効と認めた端末ＩＤと公開鍵とのペアを記憶する認定端末記憶手段22とを備えている。

【００２２】図２は、この端末10の登録が行われる手順の概略を示している。端末10の製造工場は、端末登録装置20と秘密フレーズを共有し、出荷する端末10の秘密フレーズ記憶手段11に、この秘密フレーズを格納する。ユーザ等がこの端末10を最初に利用するとき、キーペアが自動生成され、登録要求のための登録要請データがオンラインで端末登録装置20に送信される。端末登録装置20は、審査において、端末10が秘密フレーズを知っていることを確認すると、端末ＩＤと公開鍵とを認証端末記憶手段22に格納し、登録ＯＫを示す登録確認データを端末10にオンラインで送信する。端末10では、登録の完了を知ると、秘密フレーズ消去手段15が秘密フレーズ記憶手段11に格納された秘密フレーズを消去する。

【００２３】図３は、この端末10の登録要求の手順と、端末登録装置20の登録処理手順とをフロー図で示している。

ステップ１：端末10では、キーペア生成手段13が公開鍵と秘密鍵とからなるキーペアを生成する。

ステップ２：署名生成手段17は、端末Ｉ記憶手段12に記憶された端末ＩＤと、キーペア生成手段13が生成した公開鍵と、秘密フレーズ記憶手段11に格納された秘密フレーズとから成るデータをハッシュ関数で圧縮し、この一

方向性ハッシュ値に対して、キーペア生成手段13が生成した秘密鍵で暗号化し、署名データを生成する。

【００２４】ステップ３：端末ＩＤと、公開鍵と、ステップ２で生成した署名データとが送受信手段18に集められ、登録要請データが生成される。図４は、この登録要請データを模式的に示している。

ステップ４：送受信手段18は、この登録要請データを端末登録装置20に送信する。

ステップ５：端末登録装置20では、送受信手段23がこの登録要請データを受信する。

【００２５】ステップ６：署名検証手段24は、登録要請データから、端末ＩＤと公開鍵とを取り出し、また、秘密フレーズ記憶手段21から秘密フレーズを読み出し、端末ＩＤと公開鍵と秘密フレーズとの一方向性ハッシュ値を計算し、その値と、署名データを公開鍵で復号したときのデータとが一致しているかどうかを判定する。一致しているときは、端末10が秘密のフレーズを知っているものと判断し、

ステップ７：端末ＩＤと公開鍵とのペアを認証端末記憶手段22に格納し、

ステップ８：送受信手段23から、登録完了を示す登録確認データを端末10に返信する。

【００２６】ステップ９：端末10では、送受信手段18が端末登録装置20から返信された登録確認データを受信し、

ステップ10：この登録確認データが登録完了を示す情報である場合に、キーペア生成手段13が生成したキーペアをキーペア格納手段14に格納し、

ステップ11：秘密フレーズ消去手段15が、秘密フレーズ記憶手段11に格納されている秘密フレーズを消去する。

【００２７】また、端末登録装置20は、ステップ６において、データが一致していないときは、登録を拒否する。

【００２８】なお、キーペア格納手段14は、キーペアのうち、秘密鍵だけを外部から参照できない場所に格納するものであっても良い。

【００２９】このように、端末登録装置20は、端末10が秘密フレーズを知っている場合に、特定の工場の製品であると判断し、その端末10のＩＤと公開鍵とを登録する。秘密フレーズは、端末10から端末登録装置20に暗号化されて転送されるため、ネットワークを通じて秘密フレーズが漏洩する虞れは無い。また、端末10に記憶された秘密フレーズは、登録完了直後に消去されるので、ユーザが端末10を使用する段階で秘密フレーズが漏れることも無い。

【００３０】この方式では、端末登録装置20は、審査にパスした端末10に証明書は返さず、「登録ＯＫ」だけを伝える。端末10にサービスを提供するサーバは、端末10を認証するとき、毎回端末登録装置20に問い合わせることになる。

【００３１】図５は、この方式の場合に、登録を受けていない端末10がサーバのサービスを利用するときに交わされる手順を示している。

（１）端末は、端末ＩＤを提示してサーバにサービスの利用を要求すると、

（２）サーバは、端末登録装置に対して、その端末ＩＤを有する端末の認証を要求する。

（３）端末登録装置は、端末が未登録であるため、認証拒否をサーバに伝え、

（４）サーバは、端末に利用拒否を通知する。

そこで、端末は、先のステップ１～ステップ３の手順で登録要請データを生成し、

（５）端末登録装置に登録要求を行う。

（６）端末登録装置は、先のステップ５～ステップ８の手順で登録を実行する。

（７）端末が改めて、端末ＩＤを提示して、サーバにサービスの利用を要求すると、

（８）サーバは、端末登録装置に対して、その端末ＩＤを有する端末の認証を要求し、

（９）端末登録装置は、その端末の端末ＩＤ及び公開鍵に端末登録装置のデジタル署名を添えてサーバに転送する。

（10）サーバは、端末登録装置の公開鍵を用いてデジタル署名を検証し、端末のサービスの利用を許諾する。

【００３２】サーバが、端末登録装置から端末の公開鍵を受け取ったことにより、端末は、以後、生成したキーペアを用いて、サーバと暗号化した通信を行うことが可能になる。

【００３３】このように、秘密のフレーズを利用することにより、端末を他社製品と区別し、且つ、ネットワーク上で各端末を個別に識別できる形で登録することが可能になる。

【００３４】工場では、製造する端末に秘密のフレーズを記憶させる作業は必要になるが、それ以外の複雑な作業や特別の装置は必要としない。また、端末の認定は、端末登録装置20の認証端末記憶手段22に格納された該当する記録を消去することにより、端末ごとに取り消すことが可能である。

【００３５】なお、秘密のフレーズは、全社で共通のものを使用しても良く、また、工場毎、機種毎、端末ロット毎、端末毎に異なる秘密フレーズを使用しても良い。また、所定期間ごとに秘密フレーズを切り換えるようにしても良い。

【００３６】また、デジタル署名の生成や検証に使用する一方向性ハッシュ関数には、ＳＨＡ－１（Secure Hash Algorithm-1）、ＭＤ５（Mesage Digest Algorithm 5）、または両者の排他的論理和などを用いることができる。

【００３７】また、公開鍵及び秘密鍵による暗号化・復号化には、ＲＳＡ（Ronald Rivest,Adi Shamir,Leonard

Adleman）方式やＤＳＡ（Digital Signature Algorithm）方式などを使用することができる。

【００３８】端末の登録要求は、販売店の店員がサービスコードを使って実行しても良く、また、工場での製品テスト時にサービスコードを使って行っても良い。

【００３９】端末10と端末登録装置20とを結ぶ通信回線は、電話回線であってもインターネットであっても良い。

【００４０】また、登録要請データは、図６に示すように、秘密フレーズを暗号化鍵に用いて暗号化することも可能である。

【００４１】この場合、端末10の署名生成手段17は、端末ＩＤと公開鍵とから成るデータの一方向性ハッシュ値を計算し、このハッシュ値を秘密鍵で暗号化して署名データを生成する。送受信手段18は、識別ＩＤ、公開鍵、及び前記署名データ含む登録要請データを秘密フレーズで暗号化して端末登録装置20に送信する。

【００４２】端末登録装置20では、署名検証手段24が、暗号化された登録要請データを秘密フレーズで復号化し、端末ＩＤと公開鍵とを取り出して、その一方向性ハッシュ値を計算し、その値と、署名データを公開鍵で復号したときのデータとが一致しているかどうか判定する。一致していれば、端末10が秘密のフレーズを知っていることになる。

【００４３】また、端末登録装置20に登録した端末10の公開鍵は、所定の時期に更新することができる。この鍵更新は、端末側の主導で行っても、端末登録装置側の主導で行っても良い。

【００４４】この場合、端末10では、キーペア生成手段13が新公開鍵と新秘密鍵とのペアを生成し、図７に示すように、署名生成手段17が、新公開鍵と端末ＩＤとから成るデータの一方向性ハッシュ値を計算し、このハッシュ値を旧秘密鍵で暗号化して署名データ（旧署名（新公開鍵、端末ＩＤ））を生成する。そして、この署名データと新公開鍵と端末ＩＤとを含む更新登録要請データを送受信手段18から端末登録装置20に送信する。

【００４５】端末登録装置20では、送受信手段23が更新登録要請データを受信すると、署名検証手段24は、更新登録要請データから、端末ＩＤと新公開鍵とを取り出し、その一方向性ハッシュ値を計算する。また、認証端末記憶手段22から、端末ＩＤに対応する旧公開鍵を読み出し、旧署名（新公開鍵、端末ＩＤ）を旧公開鍵を復号化し、その値と、計算したハッシュ値とが一致しているかどうかを判定する。一致しているときは、正当な端末10からの更新登録要求であると判断し、認証端末記憶手段22に格納している、その端末の端末ＩＤに対応する公開鍵を新公開鍵に更新し、送受信手段23から、更新登録完了を示す更新登録確認データを端末10に返信する。この更新登録確認データを受信した端末10では、キーペア生成手段13が生成した新キーペアをキーペア格納手段14に格納する。

【００４６】このように、一旦登録した端末の公開鍵の更新についても、安全に行うことができる。端末登録装置20は、鍵の有効期間を設定して、鍵の更新を定期的に行わせることにより、登録機関としての信頼性を高めることができる。

【００４７】また、秘密フレーズは、外部から参照できない場所にＲＯＭを使って格納する場合には、消去の必要がない。また、この場合、ＲＯＭに格納した秘密のフレーズを使って公開鍵の更新を行うこともできる。

【００４８】（第２の実施形態）第２の実施形態では、端末登録装置20が、登録した端末に対して証明書を発行する場合について説明する。

【００４９】図８は、登録を受ける端末10と、端末を登録する端末登録装置20との構成を示している。端末登録装置20は、証明書を生成する生成手段25を備え、端末10は、証明書を記憶する記憶手段19を備えている。その他の構成は第１の実施形態（図１）と変わりがない。

【００５０】図９は、この端末10の登録要求の手順と、端末登録装置20の登録処理手順とをフロー図で示している。ステップ21～ステップ27及びステップ34の手順は、第１の実施形態（図３）のステップ１～ステップ７及びステップ12の手順と変わりがない。署名検証手段24は、登録要請データに含まれる署名を検証すると（ステップ26）、端末ＩＤと公開鍵とのペアを認証端末記憶手段22に格納し（ステップ27）、また、端末ＩＤと公開鍵とを証明書生成手段25に出力する。

ステップ28：証明書生成手段25は、その端末ＩＤと公開鍵とから成るデータの一方向性ハッシュ値を計算し、このハッシュ値を端末登録装置20の秘密鍵で暗号化して端末登録装置20の署名データを生成し、端末ＩＤと公開鍵とともに送受信手段23に出力する。

【００５１】ステップ29：送受信手段23は、端末ＩＤと、公開鍵と、両者に対する端末登録装置20の署名データとを含む証明書を端末10に送信する。

ステップ30：端末10では、送受信手段18が端末登録装置20から送信された証明書を受信すると、

ステップ31：証明書記憶手段19が証明書を格納し、

ステップ32：キーペア生成手段13が生成したキーペアをキーペア格納手段14に格納し、

ステップ33：秘密フレーズ消去手段15が、秘密フレーズ記憶手段11に格納されている秘密フレーズを消去する。

【００５２】図１０は、この方式の場合に、登録を受けていない端末10がサーバのサービスを利用するときに交わされる手順を示している。

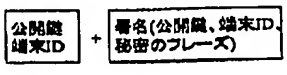
（１）端末は、端末ＩＤを提示して、サーバにサービスの利用を要求する。

（２）サーバは、この利用要求に端末登録装置の証明書が添付されていないため、端末を認証することができず、端末の利用要求を拒否する。

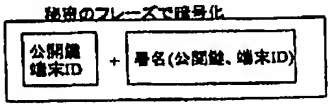
【００５３】そこで、端末は、先のステップ21～ステップ23の手順で登録要請データを生成し、
（３）端末登録装置に登録要求を行う。
（４）端末登録装置は、先のステップ25～ステップ29の手順で登録を実行し、証明書を発行する。
（５）端末は、改めて、端末ＩＤに証明書を添えてサーバにサービスの利用を要求する。
（６）サーバは、証明書を端末登録装置の公開鍵を用いて検証し、端末のサービスの利用を許諾する。
【００５４】このように、端末は、端末登録装置が発行した証明書を用いてサーバの認証を受けることができる。また、端末登録装置は、発行した証明書が長期間に渡って更新されないまま使用されることを防ぐため、証明書失効リストを作成してサーバに配布する。サーバは、端末から利用要求があったとき、失効した証明書に基づく認証を拒否する。これを受けて端末は、端末登録装置に対して、第１の実施形態（図７）で説明した鍵の更新手続きを行い、鍵の更新と合わせて更新された証明書を取得する。
【００５５】本発明の端末登録方法は、通信機能を備えた、電話機、ＦＡＸ，コピー機、テレビ、ビデオ、ＳＴＢ、冷蔵庫、電子レンジ、ＩＣカード、ＰＣ、プリンタ、ジャーポット、食器洗い機、洗濯機、湯沸かし機、照明、自動ドア、自販機、エレベータ、ゲーム機、音楽再生装置、扇風機、エアコン、ヒーター、ガスコンロ、自転車、車、バイク、カーナビ、掃除機、アイロン、あるいはそれらの複合機などの端末を対象として、広く適用することができる。
【００５６】また、本発明の端末及び端末登録装置における構成は、ハードウエアで実現しても、または、コンピュータの動作を規定するプログラムで、コンピュータを端末及び端末登録装置の機能を実行するように動作させて実現しても構わない。
【００５７】
【発明の効果】以上の説明から明らかなように、本発明の端末登録システムと、その装置及び方法では、製造された端末を、他社製品と区別して、且つ、ネットワーク上で個別に識別できるように登録することができる。
【００５８】また、この登録システムは、工場での装置や作業量の増大を伴うこと無く、効率的に実施でき、また、不正の混入を防ぎ、安全に登録することができる。
【００５９】また、端末を個々に指定して認定の取り消＊しを行うことも可能である。

【図面の簡単な説明】
【図１】第１の実施形態におけるシステムでの端末及び端末登録装置の構成を示すブロック図、
【図２】第１の実施形態のシステムでの登録手順の概要を説明する図、
【図３】第１の実施形態のシステムでの処理手順を示すフロー図、
【図４】第１の実施形態のシステムでの登録要請データのデータ構成を示す図、
【図５】第１の実施形態のシステムでの認証手順を示すシーケンス、
【図６】第１の実施形態のシステムでの登録要請データの第２のデータ構成を示す図、
【図７】第１の実施形態のシステムでの更新登録要請データのデータ構成を示す図、
【図８】第２の実施形態におけるシステムでの端末及び端末登録装置の構成を示すブロック図、
【図９】第２の実施形態のシステムでの処理手順を示すフロー図、
【図１０】第２の実施形態のシステムでの認証手順を示すシーケンス、
【図１１】従来のＷｅｂブラウザ用証明書取得手順を示す図、
【図１２】従来のＩＣカードへのキーペア登録手順を示す図である。
【符号の説明】
10　端末
11　秘密フレーズ記憶手段
12　端末ＩＤ記憶手段
13　キーペア生成手段
14　キーペア格納手段
15　秘密フレーズ消去手段
17　署名生成手段
18　送受信手段
19　証明書記憶手段
20　端末登録装置
21　秘密フレーズ記憶手段
22　認定端末記憶手段
23　送受信手段
24　署名検証手段
25　証明書生成手段

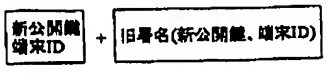
【図４】



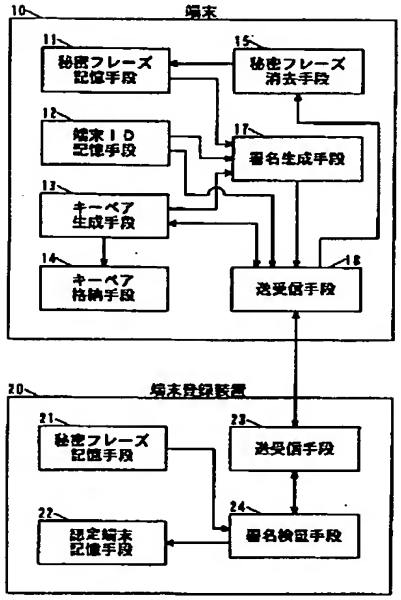
【図６】



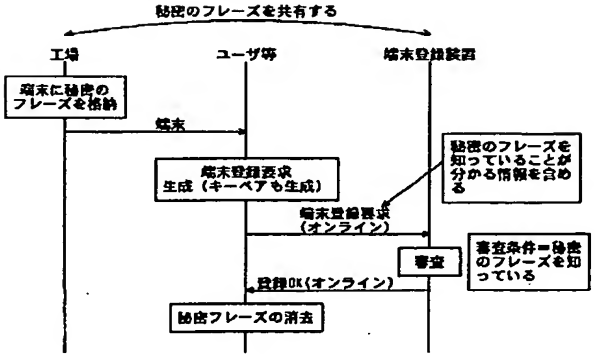
【図７】



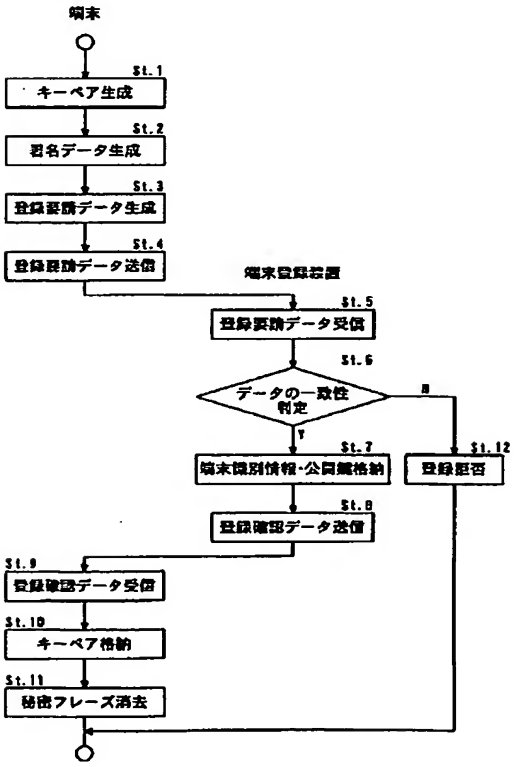
【図１】



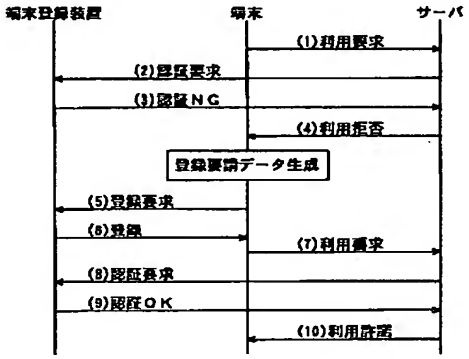
【図２】



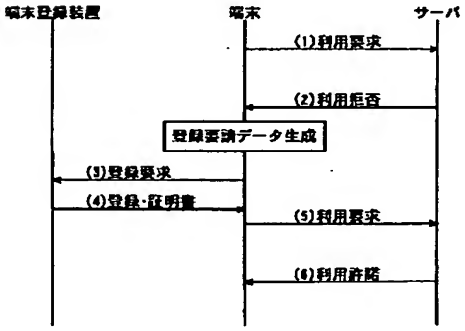
【図３】



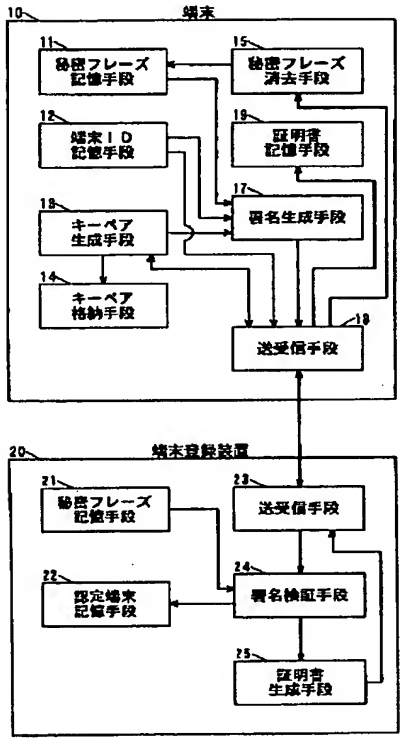
【図５】



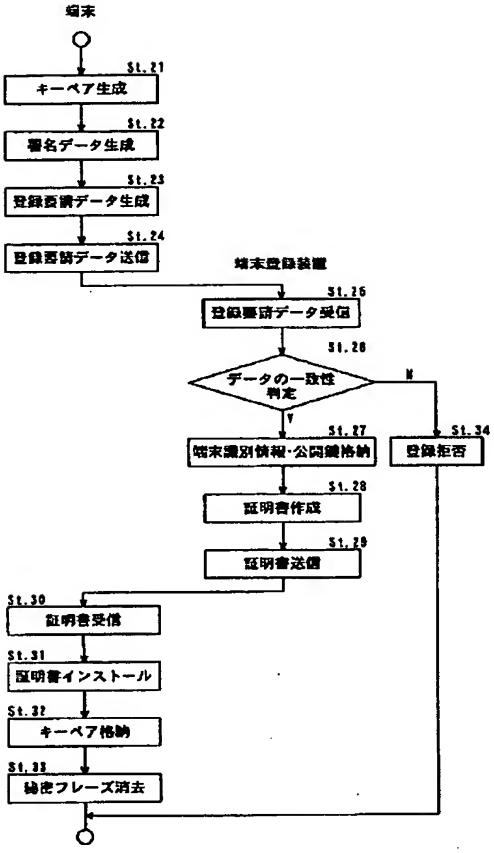
【図１０】



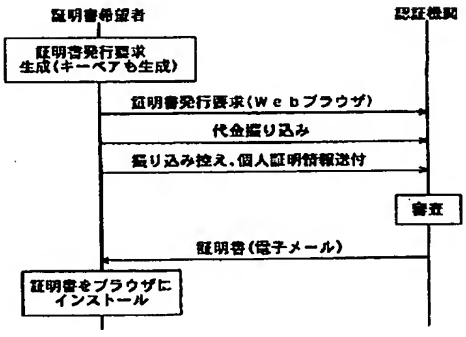
【図８】



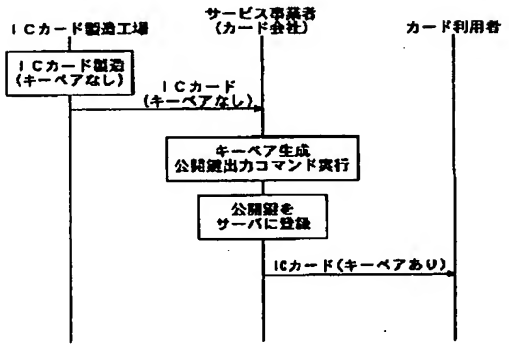
【図９】



【図１１】



【図１２】



フロントページの続き

(51)Int.Cl.[7]	識別記号	Ｆ Ｉ		ﾃｰﾏｺｰﾄﾞ(参考)
Ｈ０４Ｌ　9/00			６７５Ｂ	
			６７５Ｄ	

(72)発明者　杉浦　雅貴
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　塚本　義弘
大阪府門真市大字門真1006番地　松下電器産業株式会社内

Ｆターム(参考)　2C005 MA01 MA40 SA08 SA13
5B017 AA06 BA07 BB09 BB10 CA16
5B085 AE04 AE09 AE12 AE23
5J104 AA07 KA02 KA05 LA03 LA06
MA02 NA02 NA05 PA07